Title : Communication between a private network and a roaming mobile terminal.

Description

Field of the invention

This invention relates to communication between a private network and a roaming mobile terminal.

Background of the invention

Many organisations utilise private networks, whose communications with terminals outside the private network pass through security gateways that protect the private network using techniques including firewalls.

Protection of private corporate information is of utmost importance when designing an information infrastructure. However, the separate private networking solutions are expensive and cannot be updated quickly to adapt to changes in business requirements. The Internet, on the other hand, is inexpensive but does not by itself ensure privacy. Virtual private networking is the collection of technologies applied to a public network – in particular the Internet - to provide solutions for private networking needs. Virtual private networks use obfuscation through secure tunnels, rather than physical separation, to keep communications private.

Virtual private networks ('VPN') accordingly enable private networks to be extended to enable securitised communication with roaming terminals, that is to say terminals situated outside the private network, the communication passing for example through the Internet and possibly over mobile telephone networks. The Internet uses Internet Protocol ('IP') and the communications of mobile terminals often use Mobile Internet Protocol ('MIP').

It is expected that the roaming usage of virtual private networks will become bigger and more frequent. Such frequently roaming users will need to be given the same level of security as fixed or occasional roaming terminals, through the corporate VPN / firewall architecture.

Different communication and security protocols are used for the different networks. An example of Internet security protocol is the IPsec specification [S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", Internet Engineering Task Force (IETF), RFC 2401, November 1998]. Examples of mobile telephone communication protocols are the Mobile IPv4 specification [C. Perkins, "IP Mobility Support", RFC 2002, October 1996] and the Mobile IPv6 specification. When the VPN protocol is IPsec Encapsulating Security Payload and the mobility protocol is Mobile IP, both of them being implemented in the same IP layer, there is a need to specify how these two protocols must interact with each other when being simultaneously required.

Beyond basic application order (either apply Mobile IP first, or apply IPsec first), the overall solution must aim at meeting three major requirements:

- Security. The fact that VPN infrastructure can support Mobile-IP users must not create new security flaws to any corporate entity (corporate network & mobile or occasionally roaming users). Mobile IP enabled devices must provide mobile users with the same level of security as if they were physically located within the corporate network. On the other hand, Mobile IP entities must be adequately protected by corporate security infrastructure (Firewalls) and Mobile IP specific security mechanism must not interfere with global security mechanism.
- Compatibility. A solution that enables optimised interaction between Mobile IP and IPsec must avoid heavily modifying protocol specifications. Future evolutions of Mobile IP & IPsec protocols must not be made excessively difficult due to the use of an optimised combined solution. Optimally, such evolutions should be transparent to the use of the combined solution.
- Performance. The invention must address specific needs of mobile users in terms of handover quality: the handover must be made as quick as possible.

One example of a communication protocol for a virtual private network is the ESP (Encapsulating Security Payload) protocol (S. Kent, R. Atkinson, "IP Encapsulating Security Payload", Internet Engineering Task Force (IETF), RFC

2406, November 1998), used in tunnel mode. The most significant points are the following:

- The whole incoming IP packet is tunnelled into a new one; inner (original) source and destination addresses are not changed,
- The whole incoming IP packet is encrypted and optionally (recommended) authenticated.

ESP tunnel mode is by definition a unidirectional peer-to-peer protocol. The sender (the one that encrypts and tunnels) and the receiver (the one that detunnels and decrypts) must share a cryptographic secret (e.g. key and algorithm used for encryption/decryption). The set of security parameters (protocol, key, algorithm, sender address, receiver address, lifetime, ...) constitutes a so-called IPsec Security Association ('SA'). IPsec requires two SAs (an SA bundle) to obtain a secured unidirectional communication: one on the sender and one on the receiver (with some common parameters, for example the key).

As a VPN communication is bidirectional (from Mobile Node ('MN') to VPN Gateway and from VPN Gateway to MN), two SA bundles are required: the first one describes the tunnel from MN to VPN Gateway, the second one describes the tunnel from VPN Gateway to MN. It must be noted that the designation "VPN Gateway" is not specified by the protocol: a VPN Gateway is simply the topologic entity that terminates, at the corporate network side, all VPN secure tunnels to/from roaming mobile nodes.

SA selectors are used for the processing of IPsec packets. Basically, SA selectors are IP parameters that are used by IPsec layer to check that:

- A packet that is about to be sent on a tunnel defined by a certain outbound SA is actually legitimate to be sent with that SA (e.g. source & destination addresses of the packet match with source and destination address of the SA). This test is called the "outbound SA selector check".
- A packet that has been received from a tunnel defined by a certain inbound SA is actually legitimate to have been received with this SA (e.g. source & destination addresses of the packet match with source and destination address of the SA). This test is called the "inbound SA selector check".

It must be noted that, as illustrated in the two examples above, only source address & destination address will be considered in this invention as SA selectors for both inbound and outbound SAs.

Two families of proposals address this situation:

IPsec tunnel in the MIP tunnel.

With this family of proposals, the IPsec tunnel is established between the VPN Gateway and the Mobile Node *Home Address.*

<u>External home agent</u>. The home agent is placed in front of the IPsec gateway and the corporate firewall, i.e. outside the home network. Obviously, there are deep security flaws; the main one is that the home agent is no longer protected by the common protection (corporate firewall) mechanism at the border of the network. Indeed, a home agent placed outside the gateway does not benefit from any protection and become an easy target. This kind of security flaw could not be accepted when designing a VPN solution aimed at securing communications.

Another problem stems from the tunnelling mechanism that does not cipher the MIP packets (the IPsec tunnel is inside the MIP tunnel). The MIP header is in plain text and any attacker with bad intentions will have knowledge of all header fields, for instance the home address of the mobile node. Thus, this solution does not provide privacy and a malicious node might track all successive locations of a mobile node, identified through its home address.

<u>MIP proxy</u>. This proposal is described in a draft (F. Adrangi, P. Iyer, "Mobile IPv4 Traversal across VPN or NAT & VPN Gateway", IETF work in progress draft-adrangi-mobileip-natvpn-traversal-01.txt, February 2002). It assumes the creation of a new entity called a *Mobile IP Proxy* that appears as a surrogate home agent from a mobile node point of view and conversely is viewed as a mobile node by the home agent. This solution is also based on IPsec in MIP tunnelling, which is less confidential in terms of privacy than MIP in IPsec as stated above.

The process of simple roaming requires new signalling messages between the MIP proxy, the VPN gateway, and the home agent: the MIP proxy acts as a relay between the mobile node and the home agent ('HA'); it must be aware of existing protection between the mobile node and the HA to forward valid request uniquely. It also interacts with the VPN gateway and a common packet from a correspondent node to a MN follows a heavy process: it is first MIP-encapsulated by the HA to the MIP proxy. Then the MIP proxy decapsulates it and gives it to the VPN gateway in order to realize encryption. The VPN gateway sends back the ciphered packets to the MIP proxy, which encapsulates it again in a new MIP packet.

The MIP proxy is located outside the protected domain in the Demilitarized Zone ('DMZ'), that is to say a small network inserted as a "neutral zone" between a company's private network and the outside public network. The security level of machines within the DMZ is far inferior to the corporate network. The firewalls must not interfere with the registration procedure between the proxy and the Home Agent. This architecture implies possible security flaws since the corporate firewall must let any packets between the MIP proxy and the Home Agent go through without further inspections: this can easily lead to compromise the entire corporate network if an attacker can manage to gain access to the MIP proxy.

MIP tunnel in the IPsec tunnel

With this family of proposals, an IPsec tunnel is established between the VPN Gateway and the Mobile Node *Care-of Address*.

One proposal that includes the MIP tunnel in the IPsec tunnel has been described by the University of Bern, Switzerland at www.iam.unibe.ch/~rvs/publications/secmip_gi.pdf. The IPsec tunnel is reset before any new handover. When moving to a new network, it has to be re-established through the whole key distribution process. That handover mode creates unacceptable latencies of many seconds, incompatible with classical MIP requirements.

Another issue with this proposal consists in assuming that IPsec offers a sufficient protection and, as a consequence, in disabling authentication and replay protections during the MIP registration procedure. Disabling protections on the Home Agent is an option that does not really improve speed and requires home agents dedicated to MIP-VPN users, as well as other home agents dedicated to simple MIP users that still use MIP protections.

The present invention addresses the above and other problems.

Summary of the invention

The present invention provides a method of and apparatus for communication as described in the accompanying claims.

Brief description of the drawings

Figure 1 is a schematic diagram of a mobile virtual private network scenario.

Figure 2 is a diagram of a data packet encapsulated in ESP tunnel mode,

Figure 3 is a flow chart of exchanges in communication between a private network and a roaming mobile terminal in accordance with one embodiment of the invention, given by way of example, and

Figure 4 is a flow chart of a process for reception of a registration request in the communication process illustrated in Figure 3.

Detailed description of the preferred embodiments

Figure 1 shows a mobile virtual private network scenario comprising a private network 1 including a security gateway comprising a VPN gateway 2 and a firewall 3, a mobile node 4 situated in the private network 1 and a home agent 5 for the mobile node 4. The embodiment of the present invention shown in the drawings is applicable especially where the mobile node 4 is capable of communication over a wireless link, which improves its ability to roam, both within and outside the private network 1 but this embodiment of the invention is also applicable where the mobile node 4 communicates only over wire connections.

Figure 1 shows a scenario where the advantages of this embodiment of the invention are particularly appreciable, where the mobile node 4 moves outside the private network 1, first to a visited network 6 having a foreign agent 7 functioning under mobile IPV4 protocol, enabling communication of the roaming mobile node 4 in the network 6 through the internet 8 with the private network 1. In this scenario the roaming mobile node 4 then moves to a second visited network 9, having a foreign agent 10, also functioning under mobile IPV4 for communication through the internet 8 with the private network 1. While this embodiment of the invention functions with Mobile IPv4 protocols, it will be appreciated that the invention is also applicable to other protocols, especially the Mobile IPv6 protocol.

When the mobile node 4 is roaming in the visited networks 6 or 9, communications with the private network 1 are established through the internet 8 in IPsec and MIP tunnels 11 and 12 respectively. More specifically, the protocol used is the encapsulating security payload ("ESP") protocol illustrated in Figure 2. According to this protocol, the original packet 13 comprises an original IP header 14 and data 15. The packet 13 is encrypted with an ESP trailer 16 without changing the original IP header and destination address. The encrypted packet is encapsulated with an ESP header 17 and preferably an ESP authentication 18 and assembled with a new IP header 19 before transmission. Security association bundles, each comprising an outbound and inbound communication security association, are established for communications over the paths 11 and 12 with the VPN gateway 2. Security association selectors check that packets to be sent using the tunnel defined by each outbound security association are legitimate to be sent with that security association and, in particular, that the source and destination addresses of the packet match with the source and destination addresses of the security association, this test being the outbound SA selector check. Packets received from a tunnel defined by the inbound security association are checked for legitimacy of reception with this security association and, in particular, that the source and destination addresses of the packet match the source and destination addresses of the security association, this test being the inbound SA selector check.

In this embodiment of the invention the inbound security association of the VPN gateway 2 does not contain the IP address of the mobile node 4 as source address but a wild card ("*"). This allows the VPN gateway 2 to receive and forward a packet from the mobile node 4 whatever Care-of address it may use. It will be noted that this is not contradictory with IPsec protocol, since the wild card value is authorised by this protocol for the source address selector in a security association. The tunnel order is that of an MIP tunnel in the IPsec tunnel, with the IPsec tunnel between the VPN gateway 2 and the mobile node 4, using the mobile node Care-of address as end point.

The process for communications when the mobile node 4 is roaming is shown in Figure 3, in which references to outbound and inbound refer to packets at the mobile node 4. Initially, the IPsec tunnels are illustrated for the situation where communication is established at the current Care-of address of the mobile node 4. The outbound IPsec tunnel 20 has a security association at the mobile node 4, having the current mobile node Care-of address as source address and the address of the VPN gateway 2 as destination address, and a security association at the VPN gateway 2, having a wild card as the source address and the VPN gateway 2 address as the destination address. The initial inbound IPsec tunnel has a security association at the mobile node 4, with the address of the VPN gateway 2 as source address and the current Care-of address of the mobile node 4 as destination address, and a security association at the VPN gateway 2, having the VPN gateway address as source address and the mobile node 4 Care-of address as destination address.

When the mobile node moves at 22 from one visited network to another, for example, from the visited network 6 to the visited network 9, the mobile node 4 recognises that its location has changed, for example, from an incoming agent advertisement. It then configures a new Care-of address that is routable within the new visited network 7. The mobile node 4 contains VPN client software that responds to the change in mobile node location, for example, in response to network selection middleware or by monitoring the source addresses of outbound packets. The VPN client software then changes dynamically the inbound security association on the mobile node 4 so that its destination address is the new Care-of address of the mobile node, the inbound IPsec tunnel 21 becoming a temporary inbound IPsec tunnel 23. In this way the mobile node 4 will be able to receive packets securely sent by the VPN gateway 2 to its new Care-of address; otherwise the packets would be dropped as they would not match the destination address included in the former inbound IPsec tunnel 21. Similarly the VPN client software changes dynamically the outbound security association on the mobile node 4, so that its source address is the new Care-of address of the mobile node, the outbound IPsec tunnel 20 becoming an outbound IPsec tunnel 20'; otherwise the mobile node 4 would not be able to send outgoing packets as they would not match the source address included in the former outbound IPsec tunnel 20.

The mobile node 4 then sends a signalling message to its home agent to inform it of its new location, the signalling message passing through the outbound IPsec tunnel 20' and the VPN gateway 2. This signalling message is in the form of a registration request where the protocol used is mobile IPV4, as in this embodiment of the invention.

The signalling message is received at the VPN gateway 2 in step 24. The SA selector in the VPN gateway for the outbound tunnel 20' does not reject the packet since the source address is a wild card field and the source address is therefore not verified and the packet is forwarded to the home agent 5. At step 25 the home agent 5 receives and processes the registration request message from the mobile node 4 indicating the new Care-of address. If the registration request is valid the home agent 5 sends a security information update message ("SIU") to the VPN gateway 2 containing an order to update the security association of the temporary IPsec tunnel 23 on the VPN gateway. This SIU message is processed at the VPN gateway 2 by a daemon, for example, that is to say a background programme that provides services to the system.

In response to the SIU message the VPN gateway 2 updates its security association for the temporary inbound IPsec tunnel 23 to a new IPsec tunnel 26, having the new Care-of address of the mobile node 4 as destination address. This update is performed before any packet is sent to the mobile node 4, in particular the registration reply. In a preferred embodiment of the invention the SIU message from the home agent 5 to the VPN gateway 2 includes the registration reply to the mobile node 4.

It will be appreciated that this particular routine of the home agent 1 is triggered only when the registration request is received through a VPN gateway such as 2, corresponding to a location of the mobile node 4 outside the private network 1. If the mobile node were situated within the private network 1, and therefore not using the VPN service, the home agent 5 would respond according to the normal routine with a normal registration reply.

At step 27, the VPN gateway 2 forwards the registration reply to the mobile node 4 using the newly-established inbound IPsec tunnel 26 and sends all further data packets to the new Care-of address using the tunnel 26 until further notice.

If at step 25 the registration request does not succeed at the home agent 5, the process is not irremediably compromised. No registration reply will be received at the mobile node 4, which will send a further registration request. If the home agent 5 continues not to accept the registration requests, the mobile node 4 will ultimately abandon the attempt and establish a new tunnel for a new Care-of address without taking advantage of the process of this embodiment of the invention. This situation is inherent in mobile IP scenarios.

Figure 4 illustrates the routines followed by the home agent 5 during the above process. The routine begins at 28 and at step 29 an input is received in the form of a registration request from the mobile node 24. A check is made at step 30 whether the registration request is valid, and if the home agent 5 does not accept the registration, the routine terminates at 31. If the home agent 5 does accept the registration request, a check is made at 32 whether the registration request was received through a VPN gateway such as 2. If it was not, a registration reply is built and sent directly to the mobile node 4 over the private network 1 at step 33. If the registration request was received through a VPN gateway such as 2, a registration reply for the mobile node 4 is built at 34. This registration reply is then included in a new packet generated by the home agent 5 at 35 and which also contains the former Care-of address and the new Care-of address of the mobile node 4. That packet is then sent at step 36 to the VPN gateway 2 and the routine terminates again at 31.